REMARKS

The application is believed to be in condition for allowance.

There are no formal matters pending.

Claims 16-21 and 30-35 were rejected as obvious over KWAN 2003/0200179 in view of NOVOA 6,636,973; and claims 22-29 as obvious in further view of RUBIN et al. 6,701,522.

As was pointed out in the last response, neither of KWAN and RUBIN teaches the present invention's concept of settling a data sale using a prepaid card having a user-supplied password set after every transaction.

As recited by claim 16, a first validation of the prepaid card uses a <u>system-set first-time password number</u> stored on the database as the current password number, after each validation, <u>the user sets a new user-set password number</u> as the current password number stored in the database.

This approach provides both a convenient and elegant solution not taught or suggested by the applied art. Additionally, since only a dial-up access number to the web, a password number for the first-time use, and a serial number are indicated on the prepaid card of a real card, the card can be produced safely at a reasonable price with the user setting all subsequent password numbers.

KWAN takes an opposite approach to that of the invention; that is, KWAN uses the system to set each next

password number, e.g., codes are set by the merchant and the customer must accept the merchant-set code and later re-input the merchant-set code in order to validate the prepaid card.

See the KWAN Abstract: "This is a pre-paid card system used to store monetary value and subsequently for making payment to merchants …. Unlike static credit card numbers, this invention employs the generation of encrypted dynamic codes for each transaction, which must be verified within a specific time, for payment initiation. **Codes are send by merchant when a purchase is agreed upon and each codes have a time limit to be used.** Customers need to accept [these] codes and present them to the host computer to complete the payment process. Codes from both merchant and customer are decrypted at the host computer to produce the authenticated instructions for the payment. … ."

The Official Action offers NOVOA for teaching that, after each of plural password validations, the user set a new password number as the current password number stored in the database. The Official Action refers to NOVOA Abstract, column 2, lines 27-49; and column 3, lines 6-25.

Applicant respectfully disagrees.

The NOVOA abstract discloses a client computer coupled to a server computer that dynamically changes a user's password each time the user logs on to the computer network. NOVOA teaches using a biometrics sensing device and software and/or hardware in the client and server computers to capture a sample

from the biometrics sensing device and create a template value from the captured sample. NOVOA teaches that the template value thus is representative of a bodily characteristic of the user who activated the biometrics sensing device in an attempt to log on to the server computer. The client computer then transmits the template value to the server which compares the template value received from the client computer with template values previously stored in the users database. If a match is found, the log on process completes. At some point during or after the log on process, <u>the biometrics account manager changes the current password associated with the user to a new password and overwrites the previous password with the new password</u>.

There is no disclosure in the Abstract of the concept of the user resetting the password after each password validation.

Column 2, lines 27-49 disclose that passwords typically remain static and are only changed, if at all, after predefined periods of time to increase network security, and are normally only changed periodically. This passage teaches that it would be desirable to provide increased security. But the inventive concept discussed above is not disclosed, i.e., the inventive solution is not disclosed.

In column 3, lines 6-25 it is disclosed by NOVOA that the client computer transmits the template value to the server that includes a fingerprint matching library and a users

database. See beginning at line 15 (emphasis added). "At some point during or after the log on process, a biometrics account manager which has access to the users database changes the current password associated with the use to a new password. Thus, each time a user logs on to the computer network the password is changed, thereby increasing security in the computer network. Because the user is not required to remember and type the password, the passwords may be longer and more complex, thereby further enhancing security. In general, the passwords can be as long as is allowed by the operating system."

Also see claim 1: "1. A method … (a) capturing a biometrics sample associated with a bodily characteristic of a user; (b) generating a template value using said captured biometrics sample; (c) comparing said template value to a template value associated with a current user password stored in a database; (d) automatically changing said current user password to a new password if a match is found in step (c), and (e) storing the new password in a user database."

This is completely opposite the recited invention where the user set and inputs a new password. In NOVOA the teaching is to automate the password and to eliminate user input.

See column 2, beginning at line 51 where it is taught by NOVOA that (emphasis added) "deficiencies of the prior art described above are solved in large part by a computer network including at least one client computer coupled to a server

computer that dynamically changes a user's password preferably each time the user successfully logs on to the computer network. The server computer includes a users database …. The user attempts to log on to the server by entering a username (which is optional) and activating the biometrics sensing device to capture a sample of a bodily characteristic of the user. …. Appropriate software and/or hardware in the client and server computers capture an image of the user's fingerprint from the biometrics sensing device and create a template value from the captured image. The template value thus is representative of a bodily characteristic of the user who activated the biometrics sensing device in an attempt to log on to the server computer."

There is no input of the old password or user setting of a new password after validation. Indeed, the teaching is to rely on biometrics and to automatically generate a new password.

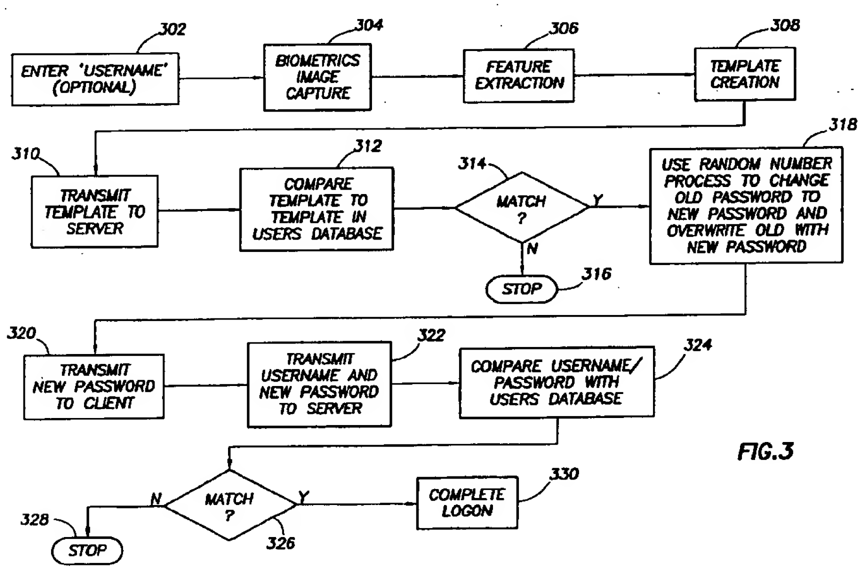

FIG.3

See Figure 3 above which clearly shows that a random number process changes the old password to a new password in step 318. Thus, NOVOA teaches automatic generation of a new password whereas the claims, e.g., claim 16 recites "after each validation, the user sets a new user-set password number as the current password number stored in the database,". There is no teaching of the user setting a new user-set password number as the current password.

Claim 16 therefore cannot be rendered obvious by NOVOA as NOVOA teaches away from the present invention.

Claim 27 recites that after validation of the prepaid card, the portal site i) requests the user to input the new user-set password number, ii) receives the new user-set password number from the user, iii) sends the received new user-set password number to the database to be stored, in the user-set password number field, as the current password number required for a next validation of the prepaid card. Attention is directed "the portal site i) requests the user to input the new user-set password number,".

NOVOA does not teach this, contrary to the position taken on page 9 of the Official Action.

As shown in Figure 3 above, NOVOA teaches the system generating a new password (step 318), informing the user of the new password (step 320), and then the user logs in with the

system-set password. This is not what is required by claim 27. Therefore, NOVOA cannot render obvious claim 27.

Claim 30 is non-obvious for the same reasons as discussed with respect to claim 16. Claim 35 is believed non-obvious for the same reasons as discussed with respect to claim 27.

In view of the above differences, reconsideration and allowance of all the claims are respectfully requested.

Applicant believes that the present application is in condition for allowance and an early indication of the same is respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/fb